IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

MELISSA STARK, on behalf of herself and all others similarly situated, Plaintiff, vs. ACUITY BRANDS, INC., Defendant.	**Civil Action File No. _____** **Complaint – Class Action** JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Melissa Stark ("Plaintiff" or "Ms. Stark"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Acuity Brands, Inc. ("Defendant" or "Acuity"). Based upon personal knowledge, information, belief, and investigation of counsel, Plaintiff specifically alleges as follows:

NATURE OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal data on a massive scale.

2. On December 7, 2021, Defendant first learned that an unauthorized

party had gained access to its computer network through two separate breaches in which cybercriminals obtained access to its systems and copied a number of files out of its network. The first breach occurred on or around October 6-7, 2020, with the second breach occurring on or around December 7-8, 2021 (collectively, the "Data Breaches"). The stolen data included current and former employee names, Social Security numbers, driver's license numbers, and financial account information, as well as limited health information related to aspects of victims' employment with Acuity, such as information related to workers compensation claims or related requests for leave under the Family and Medical Leave Act (collectively, the "Private Information").

3. Defendant only recently notified Plaintiff and putative "Class" (defined below) members that the Data Breaches involved this highly sensitive employee data.[1]

4. Defendant's multiple data security failures spanning across years of time enabled the hackers to steal and misuse the Private Information of Plaintiff

[1] Defendant posted a form notice on various state attorneys general data breach websites that require entities who have lost consumer or employee information to post a notice if the breach involves one or more of their state's citizens. A sample of the notification letter can be found here: https://ago.vermont.gov/blog/2022/12/06/acuity-brands-data-breach-notice-to-consumers/ (last accessed December 14, 2022).

and Class members. These failures led to the compromise and fraudulent misuse of Plaintiff and other Class members' Private Information and placed them at a serious, immediate, and ongoing risk of continued misuse. Additionally, Defendant's failures resulted in Plaintiff and Class members incurring costs and expenses associated with the time spent and the loss of productivity addressing and attempting to ameliorate the negative impacts of the Data Breaches, as well as emotional distress associated with constant monitoring of personal banking and credit accounts and knowing their Private Information is in the hands of cybercriminals.

5. Mitigation efforts and dealing with the actual and future consequences of the Data Breaches has and/or will also create a number of future consequences for Plaintiff and Class members—including, as appropriate, reviewing records of fraudulent charges for services billed but not received, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, the loss of property value of their personal information, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breaches.

6. The Data Breaches were caused and enabled by Defendant's violations of its obligations under statutory and common law to abide by best

practices and industry standards concerning the security of employees' records and highly sensitive information. Defendant failed to comply with security standards and allowed its employees' Private Information to be compromised, which compromise could have been prevented.

7. Accordingly, Plaintiff asserts claims for negligence, breach of contract, breach of implied contract, unjust enrichment/quasi-contract, and breach of fiduciary duty; Plaintiff also seeks injunctive relief, monetary damages, statutory damages, as well as all other relief as authorized in equity or by law.

JURISDICTION AND VENUE

8. Acuity's corporate offices are located at 1170 Peachtree St. NE, Suite 2300, Atlanta, Georgia 30309.

9. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA") because (a) there are 100 or more class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

10. The Court has personal jurisdiction because Defendant's principal place of business is located in this District.

11. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because

Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

12. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Plaintiff's and Class members' claims also occurred in this District.

PARTIES

A. Plaintiff Melissa Stark

13. Plaintiff Melissa Stark is a citizen and resident of New Ross, Indiana. Plaintiff Stark was an employee of Acuity from May to December 2019. In order to obtain employment at Acuity, Ms. Stark was required to provide her Private Information to Defendant. Defendant expressly and impliedly promised to safeguard Plaintiff Stark's Private Information but failed to do so, leading to its exposure as a direct result of Defendant's inadequate data security measures.

14. In or about early December of 2022, Plaintiff Stark received a notification letter from Defendant alerting her to the Data Breaches and that her Private Information was compromised by cybercriminals, which Private

Information included "names, Social Security numbers, driver's license numbers, and financial account information, as well as limited health information related to aspects of victims' employment with Acuity[.]"

15. The letter also offered enrollment of IdentityWorks protection service, which was and continues to be woefully inadequate. In the months and years following the Data Breaches, Plaintiff Stark and the Class have and will continue to experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in employee's names without their permission, and targeted advertising without employee consent.

16. Unfortunately, in Plaintiff Stark's case these harms are not just theoretical – she has already been the victim of bank fraud impacting both her JP Morgan Chase account and her Hoosier Heartland State Bank account. These instances of fraud occurred after the initial Data Breach, one occurring in June 2021, one in approximately April of 2021, and others at other dates.

17. Plaintiff has also recently received alerts that her driver's license number, which was also impacted by the Data Breaches, is on the dark web.

18. Although Plaintiff Stark is spending time attempting to mitigate the harm the Data Breaches have had on her life, she is still unsure as to the full extent

of the Breaches and ongoing and future harm she now faces.

B. Defendant

19. Defendant, Acuity Brands, Inc., is a global company headquartered in Atlanta, Georgia.[2] Defendant marks itself as a leading industrial technology company whose brands "are some of the most respected in lighting and intelligent spaces."[3] Defendant has a global reach, with 13,000 employees worldwide, and recently reported a "strong full-year performance with record net sales" of $1.11 billion for the fiscal fourth quarter ended August 31, 2022, and a gross profit of $462.5 million in the fourth quarter of fiscal 2022.[4]

20. Acuity's corporate offices are located at 1170 Peachtree St. NE, Suite 2300, Atlanta, Georgia 30309.

FACTS

21. Acuity manages 13,000 employees worldwide, including in seven different countries.[5] As part of its operations, Defendant stores a vast amount of its employees' Private Information. In doing so, Defendant was entrusted with, and

[2] *Acuity, Who We Are*, https://www.acuitybrands.com/who-we-are (last accessed December 14, 2022).
[3] *Id*.
[4] https://www.investors.acuitybrands.com/news-releases/news-release-details/acuity-brands-reports-fiscal-2022-fourth-quarter-and-full-year (last accessed December 14, 2022).
[5] *Id*.

obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

22. In or about December of 2022, Plaintiff Stark was informed that an unauthorized third party gained access to her former employer's network. Despite sending out notification letters to employees, Defendant has not yet articulated in detail the extent of the Breaches, the identity(ies) of the cybercriminal(s) who carried out the attacks on its network, or how the compromised information may have been used.

23. Upon information and belief, the Data Breaches exposed the Private Information of over 37,000 individuals' information stored on Defendant's servers, including that of Plaintiff and members of the Class.

24. Defendant first notified current and former employees via written letter on or around early December 2022—approximately a year after it first identified the Data Breaches on December 7, 2021. These notice letters stated that files accessed by the unauthorized third party included: "names, Social Security numbers, driver's license numbers, and financial account information, as well as limited health information related to aspects of victims' employment with Acuity, such as information related to workers compensation claims or related requests for leave under the Family and Medical Leave Act[.]"

25. On information and belief, Defendant has yet to affirmatively notify all impacted employees individually regarding what specific kind of data were stolen; nor has Defendant obtained a final count of all those impacted by the Data Breaches.

26. The Data Breaches occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated public warnings to global workplaces about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past. Defendant did not properly contain employee data, which requires a heightened level of protection. Defendant failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard employees' personal data, and in fact falsely represented that its security measures were sufficient to protect the Private Information in its possession.

27. Had Plaintiff known that her Private Information would be stored by Acuity using improper and inadequate security measures, she would have reevaluated what information she chose to provide to Defendant, which collects and stores the data of thousands of employees.

28. Defendant's failure to timely provide formal notice of both Breaches to Plaintiff and Class members exacerbated the injuries resulting therefrom.

29. Defendant was aware of or should have been aware of the risk data breaches are to global employers, which have had well-publicized breaches from misuse or misconfigurations over recent years.

30. Defendant operates a major global workplace, yet it inexplicably did not allocate adequate resources for cybersecurity protection of employee information.

31. Ponemon Institute, an expert in the annual state of cybersecurity, has indicated that 2021 had the highest average cost of data breaches in the past 17 years.[6]

A. Damages to Plaintiff and the Class Resulting from the Data Breaches

32. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breaches.

33. The Private Information obtained by hackers and scammers is an extremely valuable commodity that is commonly traded on the black market and results in the diminishment of the value of a person's electronic presence years into

[6] IBM Security, *Cost of a Breach Data* Report, PONEMON INST. (2021), https://www.ibm.com/security/data-breach.

the future when it is misused.

34. Plaintiff and the Class have experienced or currently face a substantial risk of fraudulent misuse of their Private Information, including but not limited to, loss of funds from bank accounts, fraudulent charges on credit cards, targeted advertising, suspicious phones calls, and other similar forms of identity theft.

35. In fact, Plaintiff has already suffered multiple fraudulent transactions on her bank accounts since January 2021. Each time, she was charged a "service fee" by her bank for the investigation of those fraudulent charges.

36. Plaintiff and Class members have also suffered a loss of the property value of their Private Information when it was acquired by cyber thieves in the Data Breaches. Numerous courts have recognized the propriety of the loss of the property value of personal information in data breach cases.

37. Members of the Class have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

38. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.

39. Similarly, the FTC cautions that identity theft wreaks havoc on

consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[7]

40. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, loans, or even giving false information to police during an arrest. Private Information can be used to submit false insurance claims, obtain prescription drugs or get medical treatment in the victim's name. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit and tax filings for an indefinite duration.

B. The Value of Privacy Protections and Private Information

41. The fact that Plaintiff and Class members' Private Information was

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number[.]" *Id*.

stolen—and is likely presently being offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

42. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[8]

43. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[9]

44. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

---

[8] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[9] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*] (last visited Oct. 1, 2021).

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[10]

45. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[11] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

46. Employees place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[12]

---

[10] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[11] *Web's Hot New Commodity*, *supra* note 10.

[12] *Victims of Identity Theft*, *supra* note 13, at 7.

47. At relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the manufacturing industry.

48. Had Defendant followed industry guidelines by adopting security measures recommended by experts in the field, Defendant would have prevented intrusion into its systems and, ultimately, the theft of its employees' Private Information.

49. Given these facts, any institution that transacts business with employees and then compromises the privacy of employees' Private Information has thus deprived employees of the full monetary value of their transaction.

50. Due to the actions and inactions of Defendant as such relate to Defendant's lax data security practices, procedures, and protocols, Plaintiff and the other Class members now face a greater risk of continuous identity theft due to cybercriminals' (a) recognition of this same value, and (b) intent to misuse the compromised Private Information in order to capitalize thereon. In fact, darknet

markets generate millions in revenue selling stolen personal data.[13] Ars Technica recently found "several thousand vendors selling tens of thousands of stolen data products on 30 darknet markets."[14]

CLASS ACTION ALLEGATIONS

51. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

52. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23 on behalf of a Nationwide Class defined as:

> All persons whose Private Information was compromised as a result the October 2020 data breach and/or the December 2021 data breach, both of which were discovered by Acuity Brands, Inc. on or around December 7, 2021.

53. In addition, and/or in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims on behalf of the following subclass (the "Indiana Subclass"):

> All residents of Indiana whose Private Information was compromised as a result the October 2020 data breach and/or the December 2021 data breach, both of which

[13] https://arstechnica.com/tech-policy/2022/12/darknet-markets-generate-millions-in-revenue-selling-stolen-personal-data/ (last accessed December 14, 2022).
[14] *Id*.

were discovered by Acuity Brands, Inc. on or around December 7, 2021.

54. The Nationwide Class and Indiana Subclass are collectively defined herein as the "Class."

55. Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

57. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all class members would be impracticable. On information and belief, the Nationwide Class number in the thousands.

58. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security systems prior to and during the Data Breaches complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Data Breaches were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breaches after it first learned of same;

e. Whether Defendant disclosed Plaintiff's and Class members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Private Information;

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and Class members' Private Information;

h. Whether Defendant was unjustly enriched by its actions; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries

are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

59. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breaches alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

60. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because her interests do not conflict with the interests of the Class she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

61. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

62. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or, Alternatively, the Indiana Subclass)

63. Plaintiff fully incorporates by reference all of the above paragraphs, as though they are fully set forth herein.

64. Upon Defendant accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected.

65. Defendant owed a duty of care not to subject Plaintiff and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

66. Defendant owed numerous duties to Plaintiff and the Class, including the following:

i. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;

ii. To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

iii. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

67. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard

information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, despite the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff and Class members' Private Information and misuse the Private Information and intentionally disclose it to others without consent.

68. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized employer data breaches similar to the Data Breaches that are the subject of this Complaint.

69. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

70. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

71. Because Defendant knew that a breach of its systems would damage

thousands of its employees, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

72. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations and common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

73. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

74. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes industry standards described herein, but also because Defendant is bound by industry standards to protect confidential Private Information.

75. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's

misconduct included failing to: (1) secure Plaintiff's and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent these types of data breaches.

76. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breaches. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

i. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

ii. Failing to adequately monitor the security of Defendant's networks and systems;

iii. Allowing unauthorized access to Class members' Private Information; and

iv. Failing to timely notify Class members about the Data Breaches so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

77. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its

duty to use reasonable care to adequately protect and secure Plaintiff and Class members' Private Information during the time it was within Defendant's possession or control.

78. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

79. Neither Plaintiff nor the other Class members contributed to the Data Breaches and subsequent misuse of their Private Information as described in this Complaint.

80. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

81. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the Indiana Subclass)

82. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

83. Defendant, as employer, held the Private Information on behalf of Plaintiff. Holding Plaintiff and Class members' Private Information was part of Defendant's regular business practices, as agreed by the parties. When Plaintiff and Class members joined Defendant's employment, they agreed to have their Private Information stored in Defendant's network.

84. Plaintiff and Class members entered into employment contracts with Defendant in which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. Plaintiff and Class members were required to share Private Information to obtain employment. In entering into such contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

85. Plaintiff and Class members fully performed their obligations under their employment contracts with Defendant.

86. Defendant breached the employment contracts it entered into with

Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the Data Breaches and notify Plaintiff and Class members thereof within a reasonable time.

87. As a direct and proximate result of Defendant's breaches of its employment contracts between it and Plaintiff and Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

88. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the Indiana Subclass)

89. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

90. Plaintiff brings this claim in the alternative to her breach of contract claim.

91. Defendant, as employer, held the Private Information on behalf of Plaintiff. Holding Plaintiff and Class members' Private Information was part of

Defendant's regular business practices, as agreed by the parties. When Plaintiff and Class member's joined Defendant's employment, they agreed to have their Private Information stored in Defendant's network.

92. Plaintiff and Class members entered implied contracts with Defendant in which Defendant agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. Plaintiff and Class members were required to share Private Information to obtain employment. In entering such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant and its subsidiaries' data security practices complied with relevant laws and regulations and were consistent with industry standards.

93. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

94. Defendant breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the Data Breaches within a reasonable time.

95. As a direct and proximate result of Defendant's breaches of the implied contracts between them and Defendant, Plaintiff and Class members sustained actual losses and damages as described in detail above.

96. Plaintiff and Class members are also entitled to injunctive relief

requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT IV
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of the Nationwide Class or, Alternatively, the Indiana Subclass)

97. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

98. Plaintiff and Class members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiff and Class members should have been entitled to have Defendant protect their Private Information with adequate data security.

99. Defendant knew that Plaintiff and Class members conferred a benefit on Defendant and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff and Class members' Private Information for business purposes.

100. Defendant failed to secure Plaintiff and Class members' Private

Information and, therefore, did not fully compensate Plaintiff and Class members for the value that their Private Information provided.

101. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate security practices previously alleged.

102. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate security, they would have made alternative employment choices that excluded Defendant or that would have limited the information entrusted to Defendant.

103. Plaintiff and Class members have no adequate remedy at law.

104. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

105. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of the Nationwide Class or, Alternatively, the Indiana Subclass)

106. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

107. Defendant had a fiduciary duty to safeguard employee Private information, which included that of Plaintiff and Class members.

108. Defendant breached this duty when it did not protect Plaintiff's and Class members' Private Information.

109. Defendant breached this duty when it did not provide adequate and timely notification of the Data Breaches to Plaintiff and Class members.

110. Plaintiff and Class members face injuries as a direct and proximate result of Defendant's breaches of its fiduciary duties. These injuries include, but are not limited to:

i. Actual misuse of their compromised Private Information;

ii. Loss of control over Private information;

iii. Compromise of Private Information;

iv. Lost opportunity costs associated with time spent to protect themselves and mitigate harm;

v. Continued risk that Plaintiff and Class members Private Information could be stolen and misused again;

vi. Future costs associated with time spent protecting themselves from future harm;

vii. Diminished value of Defendant's services;

viii. Diminished value of Private Information; and

ix. Anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT VI
DECLARATORY/INJUNCTIVE RELIEF
(On Behalf of the Nationwide Class or, Alternatively, the Indiana Subclass)

111. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

112. This court is authorized under 28 U.S.C. § 2201 *et seq.* to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the state statutes described in this Complaint.

113. An actual controversy has arisen in the wake of the Data Breaches regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise

their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

114. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employee Private Information.

115. Defendant still possesses the Private Information of Plaintiff and the Class.

116. Defendant has made no announcement that it has changed its data storage or security practices related to the Private Information.

117. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breaches.

118. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Acuity. The risk of another data breach is very real, immediate, and substantial.

119. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Acuity, Plaintiff and Class Members will

likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

120. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Acuity, thus eliminating the additional injuries that would result to Plaintiff and Class Members, along with other consumers whose PII would be further compromised.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class proposed in this Complaint, respectfully demands a jury trial of all issues so triable and requests that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;

B. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

C. Ordering injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members indefinitely;

D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and her counsel;

E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

JURY DEMAND

Plaintiff hereby requests a trial by jury.

Dated: December 14, 2022.

Respectfully submitted,

SHIVER HAMILTON CAMPBELL, LLC

/s/ Kyle G.A. Wallace
Kyle G.A. Wallace
Georgia Bar No. 734167

Attorneys for Plaintiff

3490 Piedmont Road, Suite 640
Atlanta, Georgia 30305
Telephone: (404) 593-0020
Facsimile: (888) 501-9536
kwallace@shiverhamilton.com

Nicholas A. Migliaccio (*pro hac vice forthcoming*)
Jason Rathod (*pro hac vice forthcoming*)
Tyler Bean (*pro hac vice forthcoming*)
MIGLIACCIO & RATHOD, LLP
412 H Street NE
Washington, D.C. 20002
202.470.3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com
tbean@classlawdc.com